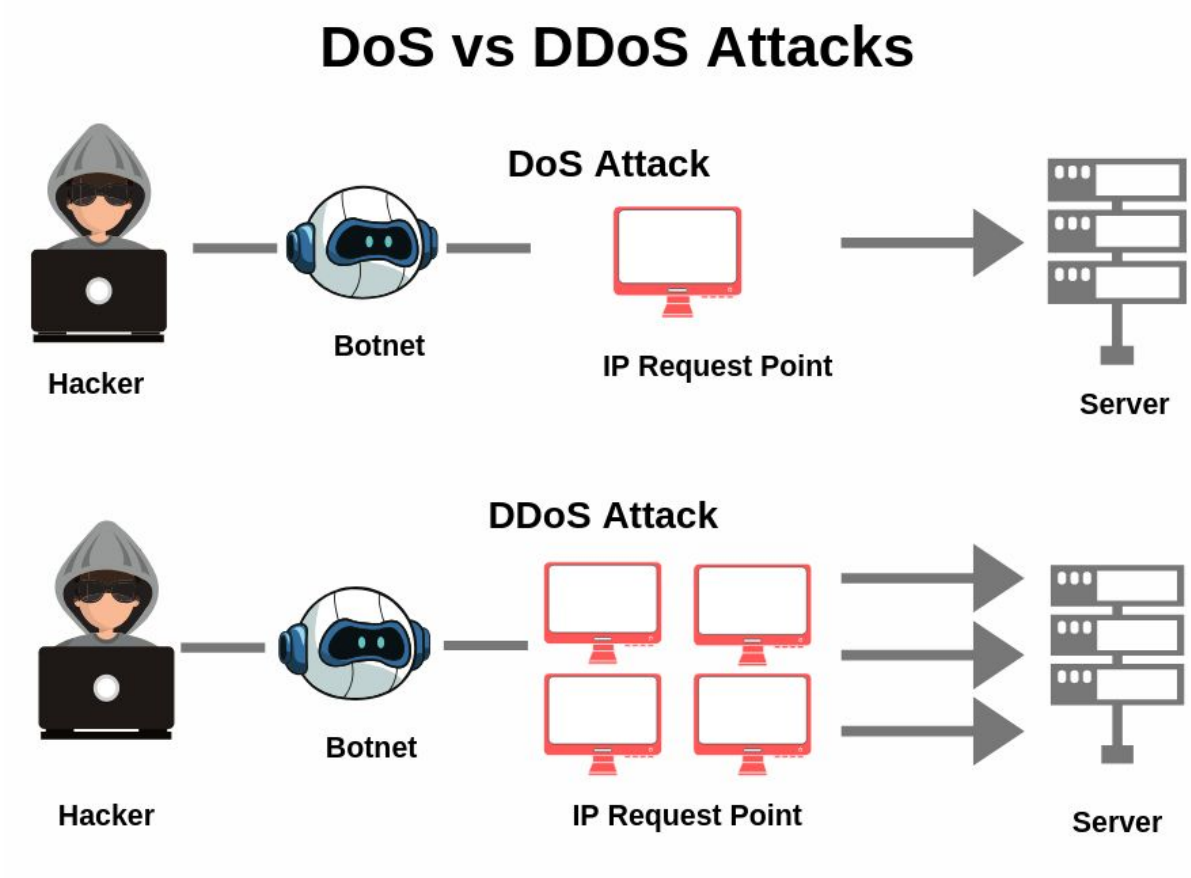
Защита от DoS и DDoS атак

Принципы и методы защиты

Основные понятия

Веб-серверы могут обрабатывать только ограниченное количество запросов одновременно. Кроме того, есть ограничения на скорость передачи данных между сервером и интернетом. Когда число запросов превышает возможности любого компонента системы, веб-сайт может полностью перестать работать. Это называется отказом в обслуживании или Denial-of-Service (коротко DoS).

DDoS-атака, или Distributed Denial of Service, — это распределенная атака типа «отказ в обслуживании».


DoS vs DDoS Attacks
DoS Attack
Hacker
Botnet
IP Request Point
Server
DDoS Attack
Hacker
Botnet
IP Request Point
Server

Инструменты DDoS-атак

На черном рынке есть масса инструментов, которые злоумышленники могут использовать для проведения атак. Одним из самых известных является Mirai — ботнет, который заражает плохо защищенные устройства: маршрутизаторы и камеры наблюдения.

Популярны также LOIC и HOIC, которые позволяют отправлять множество запросов на серверы и настраивать атаки. В даркнете можно найти и сервисы аренды ботнетов, которые позиционируются как инструменты для тестирования сетей, но иногда используются для DDoS-атак.

Часто применяются Xerxes и Slowloris. Первый перегружает серверы веб-запросами, а второй отправляет неполные HTTP-запросы и удерживает соединение открытым. Это истощает ресурсы сервера и приводит к отказу в обслуживании.

Большинство инструментов легко найти на форумах и в даркнете, поэтому DDoS-атаку может совершить человек даже без глубоких технических знаний.

Цели DDoS-атак

Главная цель DDoS-атаки — сделать ресурс недоступным для пользователей. Помимо полного отказа системы, в результате атаки могут возникнуть следующие проблемы: существенное замедление времени ответа на запросы и невозможность обработки части запросов.

Мотивация у злоумышленников может быть разной. Некоторые делают это ради забавы или для того, чтобы показать свои хакерские навыки. Чаще же атаки используются для вымогательства денег или для причинения вреда конкурентам: злоумышленники могут требовать определенную сумму в обмен на обещание прекратить атаку.

Бывают случаи, когда атаки происходят ненамеренно. Так, бездумный скраппиинг данных или мониторинг изменений веб-сайта может привести к DDoS-атаке или просто создать слишком большую нагрузку. Например, иногда в компаниях появляются проекты динамического ценообразования через автоматическое слежение за ценами конкурентов — в результате может возрасти нагрузка на сервисы конкурентов.

Опасность DDoS-атак

Очевидно, что DDoS-атаки могут привести к значительным финансовым потерям. Компании теряют деньги из-за простоев и тратят огромные суммы на восстановление и защиту данных. Для маленьких компаний это может быть и вовсе катастрофой, после которой они не смогут восстановить свою работу и вернуть клиентов. Ведь кроме денег, компании теряют и репутацию.

Приведем несколько примеров крупнейших атак. В 2012 году американские банки Bank of America и JPMorgan Chase столкнулись с атакой мощностью 60 Гбит/с, что привело к временной недоступности онлайн-сервисов и нанесло огромный ущерб их репутации.

В 2016 году атаки ботнетом Mirai привели к временной недоступности популярных онлайн-сервисов, включая GitHub, Twitter и Netflix.

В 2017 году сервисы Google столкнулись с атакой мощностью 2.54 Тбит/с, которая стала самой мощной в истории. Атака длилась около 6 месяцев и нанесла существенный ущерб инфраструктуре компании.

DDoS-атаки также имеют социальное и политическое влияние. Атаки на правительственные сайты или средства массовой информации обычно направлены на подрыв доверия к властям или вмешательство в политические процессы. Например, в марте 2014 года произошла серия DDoS-атак на веб-сайты правительственных учреждений США, включая Белый дом и Министерство обороны.

Виды DDoS-атак

Атаки классифицируются по разным признакам: источник, цель, механизм. Если мы говорим о цели, то атаки могут быть направлены на серверы, сети, веб-сайты или на отдельных пользователей. По источнику атаки делятся на те, что происходят от компьютеров, ботнетов, и других скомпрометированных устройств в сети.

Чтобы быть готовым к DDoS-атаке, важно понимать, с чем предстоит столкнуться. Мы можем классифицировать DDoS-атаки по трем основным механизмам действия: атаки на основе флуда, атаки, которые эксплуатируют уязвимости стека сетевых протоколов и атаки на уровне приложений.

Остановимся подробнее на первой группе — атаках, направленных на переполнение канала связи. Самые распространенные виды атак здесь — это SYN flood, ICMP flood и UDP flood. SYN flood основан на переполнении очереди соединений TCP. ICMP flood посылает большое количество ICMP-запросов, а UDP flood направлен на перегрузку целевой системы за счет большого объема UDP-пакетов.

Классификация DDoS-атак

Не вдаваясь в специфические технические подробности, самые популярные DDoS-атаки можно поделить на две категории:

1. Атаки уровня инфраструктуры – когда целью злоумышленников становятся сети, маршрутизаторы и потоки данных
2. Атаки уровня приложения – когда целью злоумышленников становится представление, то есть уровень преобразования данных для человека и машины, и само приложение на уровне работы его пользовательской части

Ещё хакеры могут атаковать канал взаимодействия между приложениями или каналы обмена данными между элементами локальной сети, но это случается реже. Все эти каналы взаимодействия описаны и классифицированы в OSI — модели взаимодействия открытых систем, включающей семь уровней, от физического до упомянутого выше уровня приложений.

Классификация по уровням модели OSI

Низкоуровневые. Они происходят на L3-L4 модели OSI, то есть в районе сетевого и транспортного протокола:

- Сетевой уровень (L3): DDoS-атаки по протоколам IPv4, IPv6, ICMP, IGMP, IPsec, RIP, OSPF. Цели таких атак — в первую очередь сетевые устройства.
- Транспортный уровень (L4): воздействие по протоколам TCP и UDP.
  Цели таких атак — конечные серверы и некоторые интернет-сервисы.

Такие атаки весьма распространены. Дело в том, что стандарты интернета в делались с расчётом на то, что все участники будут добросовестно их использовать.

Например, в протоколе UDP, который работает поверх IP, информация передаётся датаграммами, и в заголовках пакета не содержится IP ни источника, ни получателя. UDP доверяет адресацию протоколу IP, поверх которого работает, а в протоколе IP эти заголовки есть, но они никак не проверяются. Соответственно, очень многие атаки основаны на том, что меняется один из IP-адресов, как правило, это IP-адрес источника. Это называется спуфингом, т.е. атакой с подменой данных одного из узлов.

Такие атаки характерны тем, что нагружают какие-то части вашей инфраструктуры, забивают канал или заполняют служебные таблицы.

Высокоуровневые. Они затрагивают уровень приложения, L7, и воздействуют по прикладным протоколам, например, HTTP. Цели таких атак — конечные серверы и сервисы.

Самые распространённые виды атак

UDP Flood

UDP работает поверх протокола IP, и там нет установки соединения как такового — данные просто отсылаются безо всякого контроля целостности. Поэтому злоумышленник может, например, подменить IP-адрес источника — рассылать пакеты со своего устройства, но делать, вид, что они приходят из других мест. Проверить это нельзя, и именно в таком виде они придут на сервер.

При такой атаке злоумышленник генерирует множество пакетов максимального размера и отправляет на сервер-жертву. Опасность в том, что даже если сервер закрыт на firewall, невозможно повлиять на фильтрацию таких данных до их получения сетевым интерфейсом. «Последняя миля» от граничного маршрутизатора до сетевого интерфейса зачастую является наиболее уязвимым местом по пропускной способности. Пакеты всё равно пойдут через ваш канал и заполнят полосу пропускания.

Что делать. Банить на сервере пакеты по IP неэффективно, потому что заголовки легко менять (вышеупомянутый спуфинг). А если вы ещё и слушаете что-то по UDP-порту, бороться с ситуацией становится особенно сложно.

Обычно сервисы, которые работают через UDP — потоковые: IPTV, голосовые серверы вроде Тимспика, игры. Есть вариант посчитать длину пакета, которую вы обычно получаете, например, для входа в игру. И настроить firewall так, чтобы в доверенные добавлялись только адреса, откуда пришли пакеты нужного размера с подходящим содержимым. Это можно сделать с помощью анализа дампа трафика, который генерирует легитимное клиентское приложение.

Также есть методы усиления (амплификации), позволяющие многократно усилить атаку. Злоумышленник рассылает совершенно нормальным серверам по всему миру запрос (например DNS запрос, который использует UDP порт 53), в котором подменяет свой адрес на адрес жертвы в заголовках. Соответственно все сервера, на которые пришел запрос, отправляют ответ не на адрес атакующего, а на адрес жертвы, который был указан в заголовках. Так как DNS-ответ намного больше запроса, то и объем данных, который приходит на сервер жертвы, зачастую весьма велик.

Если вы не работаете через UDP, его вообще можно закрыть — так делают многие провайдеры, размещая свои DNS-сервера внутри сети.

Кстати, сейчас активно внедряют новый протокол QUIC, который будет являться транспортным для HTTP3. Этот протокол работает как раз поверх UDP и, скорее всего, будет подвержен таким атакам. Пока не знаю, как с ними планируют бороться. Может, разработают какие-то подходящие инструменты.

Фрагментированный UDP Flood

У него кроме описанного выше есть дополнительное действие. Атакующий присылает на сервер жертвы пакет, но говорит, что это только часть. Сервер-жертва резервирует у себя ресурс, чтобы собрать пакет, но новые фрагменты не приходят.

Что делать. Отбрасывать пакеты, которые по ожиданиям будут слишком большого размера, чтобы не забивать вашу оперативную память.

TCP SYN Flood

У TCP есть механизм установки соединения. Сначала источник посылает SYN-запрос о том, что хочет установить соединение. Сервер-получатель отвечает пакетом SYN+ACK о том, что готов к соединению.

Источник отвечает ACK-пакетом, подтверждая получение SYN+ACK.

Соединение устанавливается, потому что обе стороны подтвердили готовность, и начинают передаваться данные.

Здесь уже есть проверка соответствия IP-адреса, поэтому подменить его не получится. Но атакующий может генерировать SYN-пакет, инициируя новую сессию с сервером-жертвой, а соединение не установить, не отправляя ACK. Такая атака переполняет таблицу соединений, вызывая падение производительности. На настоящие запросы просто не остаётся места.

Что делать. Блокировать через firewall по превышению и настраивать лимиты по количеству SYN-пакетов в секунду, которые вы ожидаете для вашего сервиса.

HTTP Flood

Направлена уже не на соединение, а непосредственно на ваш сервис, и обычно воздействует на прикладной уровень модели OSI.

HTTP Flood — это просто генерация запросов. Здесь не происходит какой-то подмены, нарушений стандартов или тому подобного. Это распределённые запросы с целью вызвать недоступность вашего веб-сервера. Банально — злоумышленник отправляет миллионы запросов по генерации главной страницы вашего сайта, и сервер просто не справляется. Это как реальное обрушение в Черную пятницу, только вызванное искусственно.

Борьба с такими атаками сильно разнится в зависимости от инфраструктуры и характера атаки. Дальше расскажу об этом подробнее.

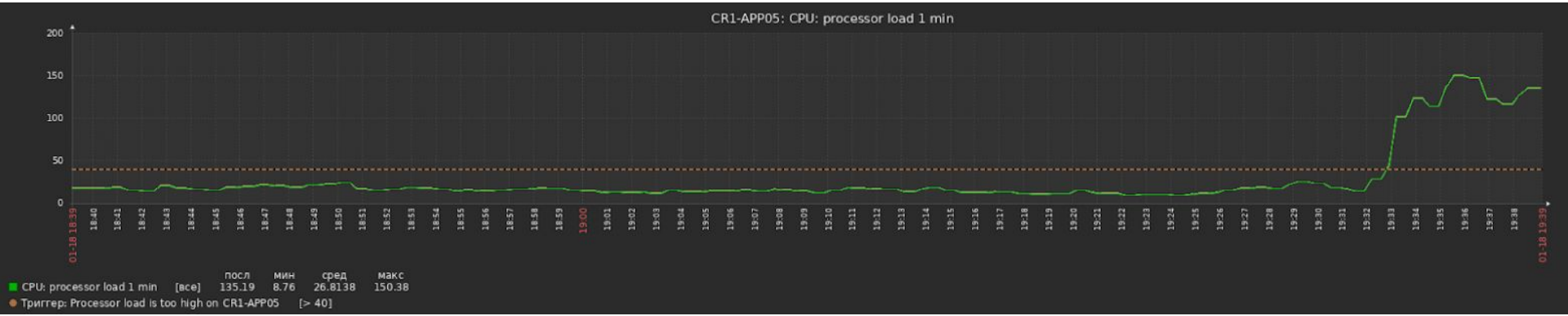
Как определить наличие DDoS-атаки

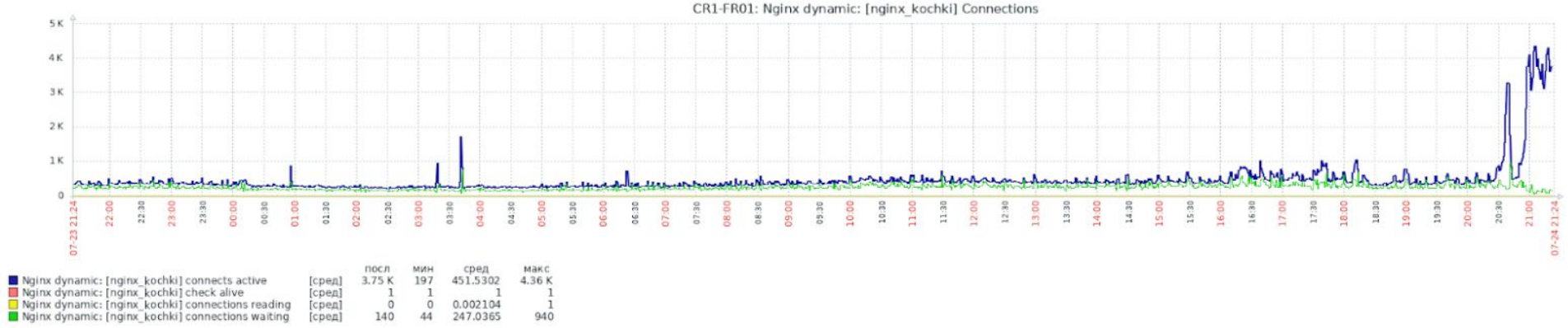
Понять, что происходит DDoS-атака, можно без особых технических знаний. Если вы заметили один или несколько из перечисленных ниже симптомов, то, вероятно, сервис стал жертвой DDoS-атаки.

Признаки DDoS-атаки:

- резко увеличился трафик без объективных причин;
- сайт замедлился или не работает;
- появились проблемы с доступом к сайту;
- пользователи сообщают о проблемах с доступом к сайту.

Кроме этих верхнеуровневых симптомов, стоит проанализировать логи и системы мониторинга трафика. Так вы сможете отследить аномалии, которые будут указывать на DDoS-атаку. Например, может обнаружиться большое количество запросов на один и тот же ресурс.
Обратите внимание на нагрузки на серверы. Если есть внезапное увеличение и сопутствующие симптомы, вероятно, это DDoS-атака. Анализ логов также поможет выявить аномальное поведение, например, многочисленные запросы с повторяющихся IP-адресов, регионов или типов устройств.


CR1-APP05: CPU: processor load 1 min
200
150
100
50
0
01.18 18:39
18:40
18:41
18:42
18:43
18:44
18:45
18:46
18:47
18:48
18:49
18:50
18:51
18:52
18:53
18:54
18:55
18:56
18:57
18:58
18:59
19:00
19:01
19:02
19:03
19:04
19:05
19:06
19:07
19:08
19:09
19:10
19:11
19:12
19:13
19:14
19:15
19:16
19:17
19:18
19:19
19:20
19:21
19:22
19:23
19:24
19:25
19:26
19:27
19:28
19:29
19:30
19:31
19:32
19:33
19:34
19:35
19:36
19:37
19:38
01.18 19:39
посл мин сред макс
CPU: processor load 1 min [все] 135.19 8.76 26.8138 150.38
Триггер: Processor load is too high on CR1-APP05 [> 40]



		посл	мин	сред	макс
Nginx dynamic: [nginx_kochki] connects active	[сред]	3.75 K	197	451.5302	4.36 K
Nginx dynamic: [nginx_kochki] check alive	[сред]	1	1	1	1
Nginx dynamic: [nginx_kochki] connections reading	[сред]	0	0	0.002104	1
Nginx dynamic: [nginx_kochki] connections waiting	[сред]	140	44	247.0365	940

Ниже команда для парсинга логов за последние 10000 и вывод в top IP адресов, встречающихся наиболее часто:

```
tail -10000 access.log | awk '{print $1}'| sort -nr | uniq -c | sort -nr | head
```

Так можно узнать количество уникальных IP, после чего можно сравнить с результатами за предыдущие сутки и узнать было ли значительное увеличение трафика:

```
cat access.log | awk '{print $1}'| sort -nr | uniq -c | wc -l
```

Следом представляем отличную команду для парсинга IP-адресов в момент фиксирования проблемы, а именно по дате и временному промежутку:

```
head access.log | grep 26/Apr/2021:1[1-2]: | awk '{print $1}'| sort -nr | uniq -c | sort -nr
```

Примеры

На простом примере рассмотрим, как может выглядеть классическая DDoS-атака. Представьте, что у вас есть некий сайт — небольшой интернет-магазин на какое-то количество товаров. Вдруг злоумышленник решает с какой-то целью нарушить работу сервиса и инициирует так называемый SYN-флуд. В процессе сервер получает огромное количество автоматических запросов на соединение, исходящих от поддельных IP-адресов. Эти запросы занимают так много места и ресурсов, что сервер перестает отвечать обычным клиентам вашего магазина, и они просто не могут попасть на сайт.

Или же другая ситуация — у вас есть крупный корпоративный сайт, представляющий известную на рынке компанию. Чтобы притормозить его работу, хакер начинает HTTP-флуд, суть которого заключается в отправке огромного количества запросов на выполнение обычных пользовательских действий — грубо говоря, сотни и даже тысячи адресов пытаются зарегистрироваться на сайте, оформить заказ, оставить отзыв или авторизоваться. Результат тот же — обычный пользователь просто не может получить доступ к нужной ему странице.

Методы защиты от DDoS-атак

Теперь поговорим о самом важном: как защитить свой сервис от DDoS-атак.

Фильтрация трафика

Используйте анти-DDoS фильтры, которые анализируют трафик в реальном времени и блокируют подозрительные запросы. Также базовые маршрутизаторы и коммутаторы часто имеют встроенные функции для фильтрации трафика на основе IP-адресов или типов протоколов.

Использование брандмауэров

Брандмауэры и файерволы помогут создать барьер между внутренней сетью компании и внешними угрозами. Их можно настроить так, чтобы они блокировали DDoS-трафик.

VPN

VPN (Virtual Private Network) создают зашифрованные туннели для передачи данных и помогают скрыть реальное местоположение серверов и затруднить DDoS-атаки. Кроме того, VPN позволяют сотрудникам безопасно подключаться к корпоративным ресурсам из любой точки мира, минимизируя риск атак на публичные IP-адреса.

CDN

CDN (Content Delivery Network) распределяет контент по множеству серверов по всему миру, что помогает снизить нагрузку на один сервер и улучшить защиту от DDoS-атак.

How does a CDN work

Content delivery without CDN

Content delivery with CDN

Предотвращение перегрузок

Arbor Peakflow и Cisco Ironport — два отличных сервиса для защиты от DDoS-атак. Первый анализирует трафик, используя данные от сетевых потоков, SNMP и обновления BGP с множества маршрутизаторов и интерфейсов, и строит логическую модель сети. Второй автоматически управляет угрозами и сетевыми аномалиями и значительно снижает нагрузку на IT-специалистов.

Выбор надежного хостинг-провайдера

Многие провайдеры предлагают встроенные решения для защиты от DDoS-атак, которые включают фильтрацию и перераспределение трафика. Также важно, чтобы хостинг-провайдер имел резервные каналы связи и мощные системы для высокой доступности сервисов.

Обратите внимание на регулярное обновление программного обеспечения и не забывайте про такие базовые вещи, как сложные пароли и двухфакторную аутентификацию.

In-house решения

В дополнение к внешним сервисам, компании могут разрабатывать собственные in-house решения для борьбы с DDoS-атаками. Сюда входят программные инструменты и скрипты, которые можно настроить под уникальные потребности и характеристики своей сетевой инфраструктуры.

Кроме того, даже обычный персонал должен иметь практические навыки, чтобы быстро распознать и отреагировать на подозрительную активность. Регулярные тренировки и симуляции помогут адекватно среагировать в момент реальной угрозы.

Что делать, если вы столкнулись с DDoS-атакой

Если вы столкнулись с DDoS-атакой, следуйте этим шагам, чтобы уменьшить ущерб и быстро восстановить доступность сервисов.

1. Сообщите администраторам и провайдеру услуг хостинга
- Как можно скорее уведомите вашу IT-команду и сетевых администраторов о подозрительной активности. Это поможет быстрее оценить ситуацию и принять меры.
- Свяжитесь с хостинг-провайдером. Многие провайдеры имеют встроенные инструменты для смягчения последствий DDoS-атак и могут быстро включить дополнительные уровни защиты.

2. Активируйте защитные механизмы и временно отключите уязвимые сервисы
- Включите все доступные защитные механизмы, WAF и сетевые брандмауэры, чтобы фильтровать вредоносный трафик.
- Временно отключите сервисы, которые являются основными целями атаки: вы снизите нагрузку на серверы и предотвратите дальнейшие сбои.
- Определите критически важные сервисы и отключите менее важные, чтобы сосредоточить ресурсы на поддержании работы самых важных систем.

3. Перенаправьте трафик на облачные хранилища
- Активно мониторьте входящий и исходящий трафик, чтобы лучше понимать характер атаки и ее интенсивность. Используйте инструменты для мониторинга сетевого, например, Arbor Peakflow.
- Перенаправьте трафик на серверы-защитники или облачные хранилища, которые могут фильтровать большой объем данных.

Схема программного фильтра от DDoS атак на сайт

Фильтр основан на том, что боты участвующие в DDoS атаках не способны выполнить JavaScript код, соответственно боты не пройдут дальше стоп-страницы фильтра, чем существенно разгрузят фронтенд/бекэнд и базу данных сайта. Т.к. на обработку каждого GET/POST запроса DDoS атаки потребуется выполнить не более 20 строк кода в бэкенде сайта и выдать страницу-заглушку объемом менее 2Кб данных.

1. Фильтр вызываем первой строкой веб-приложения, до вызова всего остального кода приложения. Так можно максимально разгрузить “железо” сервера и уменьшить объем отдаваемого трафика в сторону ботов.
2. Если посетитель попадает под условия фильтра, то выдаем посетителю специальную страницу-заглушку. На странице,
    - Сообщаем о причинах выдачи специальной страницы вместо запрошенной
    - Устанавливаем специальную куку в броузере пользователя посредством JavaScript.
    - Выполняем JavaScript код перенаправления на исходную страницу.
3. Если у посетителя установлена специальная кука, то фильтр прозрачно пропускает посетителя на запрошенную страницу сайта.
4. Если IP адрес посетителя принадлежит автономной системе из списка исключений, то трафик так же прозрачно пропускаем. Это условие необходимо для исключения фильтрации ботов поисковых систем.

Схема программного фильтра от DDoS атак на сайт

Д/з

1. Как защитить от DDoS веб-ресурс в облаке
2. user agent